PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-177523
(43)Date of publication of application : 30.06.1998

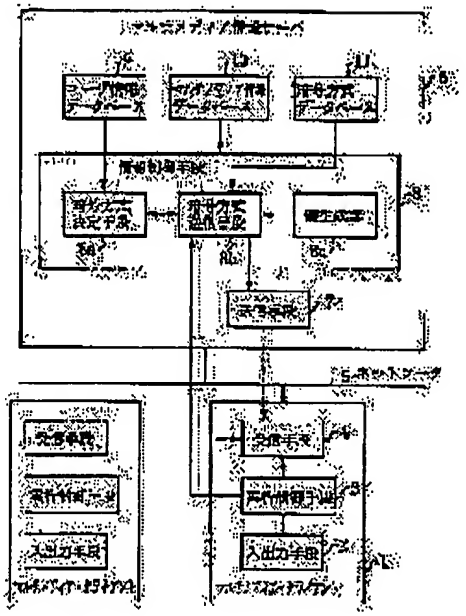
(51)Int.Cl. G06F 12/14
G06F 12/00
G06F 12/00
G09C 1/00
H04L 9/14

(21)Application number : 08-335594
(22)Date of filing : 16.12.1996

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : FUJII SEIJI

(54) MULTIMEDIA INFORMATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To guarantee the execution of multimedia information to the user of a multimedia information system based on the terms of the contract made by the user by eliminating unauthorized access to the multimedia information.
SOLUTION: A multimedia information server 6 is provided with a ciphering system deciding means 8a which decides an enciphering means which enciphers multimedia information and a decoding means which decodes enciphered multimedia information based on the terms of the contract made by a user stored in a user information database 9 and a transmitting means 7 which enciphers the multimedia information stored in the database 10 by using the enciphering means decided by the means 8a and transmits the enciphered multimedia information and a multimedia client 1 is provided with a receiving means 4 which decodes the enciphered multimedia information transmitted from the transmitting means 7 by using the decoding means decided by the deciding means 8.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－177523

(43)公開日　平成10年(1998)６月30日

(51)Int.Cl.[6]		識別記号	FI		
G06F	12/14	320	G06F	12/14	320B
	12/00	537		12/00	537H
		547			547D
G09C	1/00	660	G09C	1/00	660D
H04L	9/14		H04L	9/00	641

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）

(21)出願番号　特願平8－335594

(22)出願日　平成８年(1996)12月16日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　藤井　誠司
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

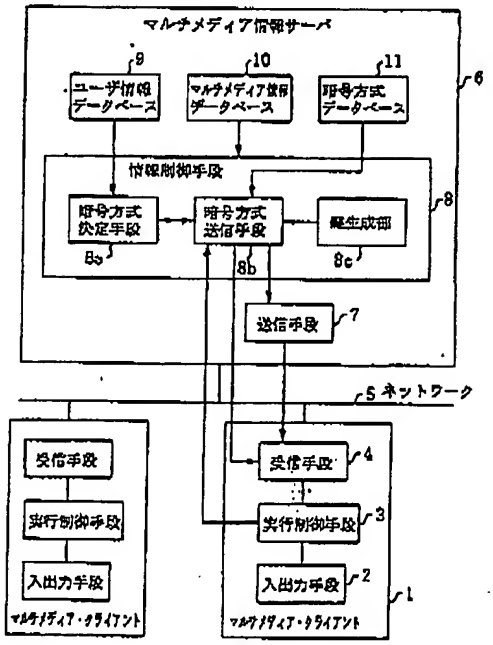
(74)代理人　弁理士　宮田　金雄　（外２名）

(54)【発明の名称】　マルチメディア情報システム

(57)【要約】

【課題】　マルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証する。

【解決手段】　マルチメディア情報サーバ６は、マルチメディア情報を暗号化する暗号化手段と暗号化マルチメディア情報を復号する復号手段とをユーザ情報データベース９に記憶されたユーザとの契約情報に基づいて決定する暗号方式決定手段８ａと、この暗号方式決定手段８ａにより決定された暗号化手段を用いて、マルチメディア情報データベース１０に記憶されたマルチメディア情報を暗号化し、この暗号化マルチメディア情報を送信する送信手段７とを備え、マルチメディア・クライアント１は、暗号方式決定手段８ａにより決定された復号手段を用いて、送信手段７により送信された暗号化マルチメディア情報を復号する受信手段４を備えた。



1

【特許請求の範囲】

【請求項1】 以下の要素を備えたマルチメディア情報システム。

（a）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（b）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（c）以下の要素を備えたサーバ；

（c1）上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；

（c2）この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（d）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

（d1）上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。

【請求項2】 それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、

上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、

上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を用いて暗号化し、

上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号することを特徴とする請求項1記載のマルチメディア情報システム。

【請求項3】 上記送信手段は、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を備え、上記暗号方式決定手段により決定された暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化し、

上記受信手段は、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を備え、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号することを特徴とする請求項1記載のマルチメディア情報システム。

【請求項4】 上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、

上記暗号方式決定手段は、上記ユーザ情報記憶手段に記憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定することを特徴とする請求項1記載のマルチメディア情報システム。

【請求項5】 上記暗号方式決定手段は、新たに決定した暗号化手段と復号手段とを送信し、

上記送信手段は、

上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、

上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、

上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、

上記受信手段は、

上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、

上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたことを特徴とする請求項1記載のマルチメディア情報システム。

【請求項6】 上記送信制御手段は、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを構築して送信し、

上記復号方式変更手段は、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させることを特徴とする請求項5記載のマルチメディア情報システム。

【請求項7】 以下の要素を備えたマルチメディア情報システム。

（a）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（b）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（c）以下の要素を備えたサーバ；

（c1）上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（c2）上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；

（d）以下の要素を備え、上記サーバに上記マルチメデ

3

ィア情報の送信を要求するクライアント；

（ｄ１）上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段；

（ｄ２）この受信手段により復号されたマルチメディア情報を実行する実行手段；

（ｄ３）この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。

【請求項８】 上記サーバは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を備え、

上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信することを特徴とする請求項7記載のマルチメディア情報システム。

【請求項９】 上記ユーザ情報記憶手段は、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶し、

上記制御手段は、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項７記載のマルチメディア情報システム。

【請求項１０】 上記マルチメディア情報記憶手段は、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶し、

上記制御手段は、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項７記載のマルチメディア情報システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、契約したユーザに文字、図形、音声、静止画又は動画からなるマルチメディア情報を暗号化して提供するマルチメディア情報システムに関するものである。

【０００２】

【従来の技術】図２０は、例えば特開平６－４４１２２号公報に示された従来のマルチメディア情報システムを示す概略構成図である。図において、５０は文字、図形、音声、静止画、動画などの各種メディアデータからなるマルチメディアファイルを暗号化して蓄積するマルチメディア情報蓄積部、５１はマルチメディア情報蓄積部５０に対するマルチメディアファイルの入出力を管理するマルチメディア情報管理部、５２はマルチメディアファイルの内容を表示する出力装置である。

4

【０００３】図２１はマルチメディア情報蓄積部５０に蓄積されるマルチメディアファイルの構成要素であるメディアデータの構成図である。図において、６０はメディアデータ、６０ａはユーザのセキュリティレベルに応じてアクセス可能なデータか否かを判別するための暗号化鍵情報、６０ｂはディスプレイ画面上での表示位置や表示する大きさを示す位置・大きさ情報、６０ｃはメディアデータのメディア種別を示すメディア種類情報、６０ｄは提示能力の異なるディスプレイ画面への対応のために入力時とは別のデータ形式のデータを付加した出力装置対応データである。このように、ユーザによるアクセスが可能か否かを判別するための暗号化鍵情報をメディアデータ毎に有しており、マルチメディアファイルを構成している一つ一つのメディアデータ単位でセキュリティレベルを変えることができる。

【０００４】次に動作について説明する。ユーザがマルチメディアファイルの出力をマルチメディア情報管理部５１に要求すると、マルチメディア情報管理部５１は、出力要求のあったマルチメディアファイルを構成しているメディアデータ６０をマルチメディア情報蓄積部５０から取り出す。次に、マルチメディア情報管理部５１は、ユーザのセキュリティレベルを解析し、各メディアデータ６０に含まれる暗号化鍵情報６０ａに基づき、そのユーザのセキュリティレベルでアクセス可能なメディアデータであるか否かを判別する。そして、ユーザがアクセス可能なメディアデータであると判別した時、このアクセス可能なメディアデータ６０のみを出力の対象とし、出力装置５２の提示能力に応じたデータ形式に変換して、出力装置５２へ出力する。

【０００５】

【発明が解決しようとする課題】従来のマルチメディア情報システムは、以上のように構成されており、暗号化したマルチメディア情報を蓄積し、ユーザへ送信している。そのため、長期間に渡って同じ暗号方式を使用することになり、契約しているユーザ以外の第三者によって通信データが盗聴され暗号方式を解読されるので、ユーザに送信しているマルチメディア情報へ第三者が不正にアクセスできるという問題点があった。

【０００６】また、ユーザのマルチメディア情報の実行に関する契約条件をマルチメディア情報を送信する前に確認するだけであり、マルチメディア情報の実行中は、ユーザが契約条件に基づいて正しく実行しているか否かがチェックできないため、マルチメディア情報を不正に実行できてしまうという問題点があった。

【０００７】また、日時、時間単位によるマルチメディア情報の実行、実行回数などの様々なユーザのマルチメディア情報の実行に関する契約条件に応じたマルチメディア情報の実行を制御することができないという問題点があった。

【０００８】この発明は、上記のような問題点を解消す

るためになされたものであり、第三者によるマルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証するマルチメディア情報システムを得ることを目的とする。

【0009】

【課題を解決するための手段】請求項1記載のマルチメディア情報システムは、以下の要素を備えたものである。

（a）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（b）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（c）以下の要素を備えたサーバ；

（c1）上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；

（c2）この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（d）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

（d1）上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。

【0010】請求項2記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を用いて暗号化し、上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号するものである。

【0011】請求項3記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を有し、上記暗号方式決定手段により決定された暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化する送信手段と、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を有し、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号する受信手段とを備えたものである。

【0012】請求項4記載のマルチメディア情報システムは、上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、上記暗号方式決定手段は、上記ユーザ情報記憶手段に記憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定するものである。

【0013】請求項5記載のマルチメディア情報システムは、新たに決定した暗号化手段と復号手段とを送信する暗号方式決定手段を備え、上記送信手段は、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、上記受信手段は、上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【0014】請求項6記載のマルチメディア情報システムは、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを搬送して送信する送信制御手段と、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【0015】請求項7記載のマルチメディア情報システムは、以下の要素を備えたものである。

（a）ユーザとの契約情報を記憶するユーザ情報記憶手段；

（b）文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

（c）以下の要素を備えたサーバ；

（c1）上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

（c2）上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；

（d）以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

（d1）上記送信手段により送信された暗号化マルチメ

ディア情報を復号する受信手段；

（ｄ２）この受信手段により復号されたマルチメディア情報を実行する実行手段；

（ｄ３）この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。

【００１６】請求項８記載のマルチメディア情報システムは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を上記サーバに備え、上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信するものである。

【００１７】請求項９記載のマルチメディア情報システムは、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶するユーザ情報記憶手段と、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。

【００１８】請求項１０記載のマルチメディア情報システムは、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶するマルチメディア情報記憶手段と、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。

【００１９】

【発明の実施の形態】

実施の形態１．以下、本発明を実施の形態に基づいて、図を参照しながら、説明する。図１は、実施の形態１のマルチメディア情報システムの構成図である。図において、１はマルチメディア情報の送信を要求するマルチメディア・クライアント、２はユーザからの要求を受け付けるとともに、マルチメディア情報の実行結果を出力する入出力手段、３はマルチメディア情報を実行し、実行結果を入出力手段２に送信する実行制御手段、４は暗号化されたマルチメディア情報を受信して復号し、実行制御手段３に送信する受信手段、５はネットワーク、６はマルチメディア情報サーバ、７はマルチメディア情報を暗号化し、マルチメディア・クライアント１へネットワーク５を経由して送信する送信手段、８は暗号方式を決定するとともに、マルチメディア情報の送信を制御する情報制御手段、９は契約しているすべてのユーザの契約情報を蓄積しているユーザ情報記憶手段としてのユーザ情報データベース、１０はマルチメディア情報サーバ６

がサービスを提供するすべてのマルチメディア情報を蓄積しているマルチメディア情報記憶手段としてのマルチメディア情報データベース、１１はマルチメディア情報サーバ６で使用できるすべての暗号方式の鍵生成手段、暗号化手段及び復号手段を蓄積している暗号方式記憶手段としての暗号方式データベースである。

【００２０】情報制御手段８は、暗号方式決定手段８ａ、暗号方式送信手段８ｂ、鍵生成部８ｃから構成されている。暗号方式決定手段８ａは、ユーザ情報データベース９に蓄積されているユーザの契約情報に基づいてマルチメディア情報を送信する時に使用する暗号方式を決定する。暗号方式送信手段８ｂは、暗号方式決定手段８ａにより決定された暗号方式の鍵生成手段、暗号化手段及び復号手段を暗号方式データベース１１から取り出し、鍵生成手段は鍵生成部８ｃへ、暗号化手段は送信手段７へ、復号手段は受信手段４へ送信する。鍵生成部８ｃは、暗号方式送信手段８ｂにより送信された鍵生成手段を用いて、暗号化鍵と復号鍵を生成する。

【００２１】本システムは、図示したように、マルチメディア情報サーバ６と、複数のマルチメディア・クライアント１とが、ネットワーク５に接続されており、マルチメディア情報サーバ６は、マルチメディア・クライアント１から要求されたマルチメディア情報をマルチメディア情報データベース１０より取り出して暗号化し、マルチメディア・クライアント１に送信するものである。

【００２２】図２は、ユーザ情報データベース９に蓄積されている契約情報の構成を示す構成図である。図において、９ａはユーザとの契約情報レコード、９ｂはユーザ登録番号、９ｃはユーザの氏名、９ｄはユーザの住所、９ｅはユーザとの契約タイプである。契約タイプ９ｅは暗号方式を決定するための情報である。

【００２３】図３は、マルチメディア情報データベース１０に蓄積されているマルチメディア情報の構成を示す構成図である。図において、１０ａはマルチメディア情報レコード、１０ｂはマルチメディア情報を一意に識別するためのマルチメディア情報番号、１０ｃはマルチメディア情報の名称、１０ｄはマルチメディア情報の実行手段を示す実行方式番号、１０ｆはマルチメディア情報である。

【００２４】図４は、暗号方式データベース１１に蓄積されている暗号方式の構成を示す構成図である。図において、１１ａは暗号方式レコード、１１ｂは暗号方式を一意に識別するための暗号方式番号、１１ｃは暗号方式の名称、１１ｄは暗号化鍵と復号鍵を生成する鍵生成手段、１１ｅはマルチメディア情報を暗号化する暗号化手段、１１ｆは暗号化されたマルチメディア情報を復号する復号手段である。

【００２５】次に動作ついて、図５のフローチャートに基づいて説明する。入出力手段２に表示されているマルチメディア情報番号１０ａとマルチメディア情報名称１

０ｃの中から、ユーザが一つのマルチメディア情報番号１０ａを選択すると（ステップＳ１）、実行制御手段３は、ユーザにより入力されたユーザ登録番号９ｂと、選択されたマルチメディア情報番号１０ａとを、マルチメディア情報サーバ６の暗号方式送信手段８ｂへ送信する（ステップＳ２）。暗号方式送信手段８ｂは、ユーザ登録番号９ｂを暗号方式決定手段８ａへ出力する（ステップＳ３）。

【００２６】暗号方式決定手段８ａは、ユーザ登録番号９ｂを検索条件としてユーザ情報データベース９からユーザの契約情報レコード９ａを取得し（ステップＳ４）、取得した契約情報レコード９ａ中の契約タイプ９ｅに基づいて暗号方式を決定し、決定した暗号方式の暗号方式番号１１ｂを暗号方式送信手段８ｂへ出力する（ステップＳ５）。

【００２７】暗号方式送信手段８ｂは、暗号方式番号１１ｂを検索条件として、暗号方式データベース１１から鍵生成手段１１ｄ、暗号化手段１１ｅ及び復号手段１１ｆを取得する（ステップＳ６）。暗号方式送信手段８ｂは、鍵生成手段１１ｄを鍵生成部８ｃへ出力し（ステップＳ７）、鍵生成部８ｃは、この出力された鍵生成手段１１ｄを使用して、暗号化鍵と復号鍵を生成し、暗号方式送信手段８ｂへ出力する（ステップＳ８）。暗号方式送信手段８ｂは、鍵生成部８ｃにより生成された暗号化鍵と、暗号方式データベース１１から取得した暗号化手段１１ｅとを送信手段７へ出力し（ステップＳ９）、鍵生成部８ｃにより生成された復号鍵と、暗号方式データベース１１から取得した復号手段１１ｆを受信手段４へ送信する（ステップＳ１０）。

【００２８】そして次に、暗号方式送信手段８ｂは、ステップＳ２で送信されたマルチメディア情報番号１０ａを検索条件として、ユーザが選択したマルチメディア情報１０ｆをマルチメディア情報データベース１０から取り出し、ブロックに分割して送信手段７へ出力する（ステップＳ１１）。送信手段７は、ステップＳ９で出力された暗号化鍵と暗号化手段１１ｅとを用いて、マルチメディア情報１０ｆの各ブロックを暗号化し、受信手段４へ送信する（ステップＳ１２）。

【００２９】受信手段４は、受信した暗号化マルチメディア情報１０ｆの各ブロックを、ステップＳ１０で送信された復号鍵と復号手段１１ｆとを用いて復号し、実行制御手段３へ送信する（ステップＳ１３）。実行制御手段３は、復号されたマルチメディア情報１０ｆを実行し、実行結果を入出力手段２へ出力する（ステップＳ１４）。

【００３０】以上のように、この実施の形態によれば、暗号方式データベース１１に蓄積されている多数の暗号方式の中から、ユーザの契約タイプに基づいて暗号方式を選択し、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、不正なアクセスが排除できるという効果がある。

【００３１】なお、この実施の形態では、暗号方式決定手段８ａが暗号方式を決定し、暗号方式送信手段８ｂが鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段８ａが暗号方式送信手段８ｂの機能を有し、決定した暗号方式に対応する各手段を送信するように構成することも出来る。

【００３２】実施の形態２．送信手段７で実行する暗号化手段や、受信手段４で実行する復号手段が変更できない場合には、図６に示すように、複数の異なる暗号方式の送信手段７と受信手段４とを用いて、情報制御手段８が送信手段７を切り替え、実行制御手段３へ同じ暗号方式の受信手段４を使用するように命令して切り替えることより、マルチメディア情報システムを実現することもできる。

【００３３】実施の形態３．また、ネットワークを経由して復号手段１１ｆを送信する場合、第三者に復号手段１１ｆを盗まれる可能性があることや、復号手段１１ｆを受信手段４へ送信する時間を短縮するため、図７に示すように、マルチメディア・クライアント側に復号手段だけを蓄積した復号手段データベース１２を分散して配置することもできる。

【００３４】実施の形態４．さらに、図８に示すように、マルチメディア情報サーバ側の送信手段７が暗号化手段データベース１３を持ち、マルチメディア・クライアント側の受信手段４が復号手段データベース１２を内部に持つように構成することもできる。

【００３５】実施の形態５．実施の形態１では、ユーザとの契約情報中の契約タイプに基づいて暗号方式を決定したが、契約タイプに合致する暗号方式の候補が複数残った場合に暗号方式を１つに決定するためには、契約タイプ以外の情報が必要になる。

【００３６】ユーザとマルチメディア情報サーバとの間で暗号化したデータを送受信するとき、使用可能な暗号方式が居住地域の法律によって制限されることがある。マルチメディア・クライアントが存在する地域で使用可能な暗号方式と、マルチメディア情報サーバが存在する地域で使用可能な暗号方式とで、まったく同じ暗号方式が使用できるとは限らないので、両方の場所で使用できる暗号方式を決定する必要があるが、これはユーザ個人との契約条件だけでは判断できない。そこで、この実施の形態では、暗号方式データベースを図９に示す構造にする。図９に示した暗号方式データベースは、図４に示した暗号方式データベースに対して、各暗号方式の使用可能地域を示す使用可能地域情報１１ｇを追加したものである。

【００３７】この実施の形態のマルチメディア情報システムの構成は、実施の形態１で説明した図１の構成と同様であるが、暗号方式決定手段８ａにおける暗号方式決定の動作が実施の形態１のものと異なる。異なる動作

は、実施の形態1で説明したステップS4、S5である。異なる動作を次に説明する。この実施の形態では、暗号方式決定手段8aは、ユーザ登録番号9bを検索条件としてユーザ情報データベース9からユーザの契約情報レコード9aを取得する。次に、図8に示した暗号方式データベース11から暗号方式レコード11aを取り出す。そして、取得した契約情報レコード9a中の住所9dが、暗号方式レコード11a中の使用可能地域情報11gに合致するか否かを調べる。合致する暗号方式が複数である場合は、その中からユーザの契約情報レコード9a中の契約タイプ9eに合致する暗号方式を決定し、決定した暗号方式の暗号方式番号11bを暗号方式送信手段8bへ出力する。

【0038】以上のように、この実施の形態によれば、ユーザの契約タイプと、暗号方式の使用可能地域情報とに基づいて暗号方式を決定するので、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択することができる。

【0039】実施の形態6．図10は、実施の形態6のマルチメディア情報システムの構成図である。図において、実行制御手段3と受信手段4は、図1に示したものと同様にマルチメディア・クライアントを構成し、送信手段7と情報制御手段8は、図1に示したものと同様にマルチメディア情報サーバを構成する。

【0040】情報制御手段8において、暗号方式決定手段8aは、暗号方式が変更になったときは、新たに暗号方式を決定し、暗号方式送信手段8bは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を図1に示した暗号方式データベース11から取り出し、鍵生成手段は鍵生成部8cへ、暗号化手段は送信手段7へ、復号手段は受信手段4へ送信する。送信手段7は、暗号方式変更手段7a、暗号化実行手段7b、7c及び送信制御手段7dから構成されている。暗号方式変更手段7aは、暗号方式送信手段8bにより送信された新たな暗号化手段に基づいて、送信手段7で使用する暗号化実行手段7b、7cを切り替える。暗号化実行手段7b、7cは、暗号方式送信手段8bから送信された暗号化手段を実行するものであり、送信制御手段7dから出力されるデータを暗号化し、その結果を送信制御手段7dへ出力する。送信制御手段7dは、情報制御手段8より出力されたマルチメディア情報のブロックを暗号化実行手段7b又は7cに出力し、暗号化実行手段7b、7cにより暗号化されたマルチメディア情報を受信手段4へ送信する。

【0041】受信手段4は、復号方式変更手段4a、復号実行手段4b、4c及び受信制御手段4dから構成されている。復号方式変更手段4aは、暗号方式送信手段8bにより送信された新たな復号手段に基づいて、受信手段4で使用する復号実行手段4b、4cを切り替える。復号実行手段4b、4cは、暗号方式送信手段8bから送信された復号手段を実行するものであり、受信制御手段4dから出力されるデータを復号して、その結果を受信制御手段4dへ出力する。受信制御手段4dは、送信制御手段7dより出力された暗号化マルチメディア情報を復号実行手段4b又は4cに出力し、復号実行手段4b、4cにより復号されたマルチメディア情報を実行制御手段3へ送信する。

【0042】次に、動作について、図11のフローチャートに基づいて説明する。暗号方式送信手段8bは、暗号方式決定手段8aにより決定された暗号化鍵と暗号化手段を暗号方式変更手段7aへ送信する（ステップS20）。暗号方式変更手段7aは、受信した暗号化鍵と暗号化手段を暗号化実行手段7bへ出力し、暗号化実行手段7bを使用して暗号化するように設定する（ステップS21）。暗号方式送信手段8bは、復号鍵と復号手段受信手段4の復号方式変更手段4aへ送信する（ステップS22）。復号方式変更手段4aは、受信した復号鍵と復号手段を復号実行手段4bへ出力し、復号実行手段4bを使用して復号するように設定する（ステップS23）。

【0043】情報制御手段8は、マルチメディア情報をブロックに分割し、送信制御手段7dへブロックを送信する（ステップS24）。送信制御手段7dは、受信したブロックを、暗号化実行手段7bへ出力する（ステップS25）。暗号化実行手段7bは、ステップS21で出力された暗号化鍵と暗号化手段を使用してブロックを暗号化し、送信制御手段7dへ出力する（ステップS26）。送信制御手段7dは、暗号化されたブロックをネットワーク5を経由して受信制御手段4dへ送信する（ステップS27）。

【0044】受信制御手段4dは、ネットワーク5から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段4bへ出力する（ステップS28）。復号実行手段4bは、ステップS23で出力された復号鍵と復号手段を使用して暗号化ブロックを復号し、受信制御手段4dへ出力する（ステップS29）。受信制御手段4dは、復号したブロックを実行制御手段3へ送信する（ステップS30）。

【0045】次に、マルチメディア情報の実行中に暗号方式を変更する場合の動作を、図12のフローチャートに基づいて説明する。情報制御手段8は、現在使用している暗号方式が変更になると、マルチメディア情報のブロックの送信制御手段7dへの送信を停止する（ステップS40）。暗号方式送信手段8bは、暗号方式決定手段8aにより決定された変更後の暗号化鍵と暗号化手段を暗号方式変更手段7aへ送信する（ステップS41）。暗号方式変更手段7aは、受信した暗号化鍵と暗号化手段を暗号化実行手段7cへ出力し、次に受信するブロックは暗号化実行手段7cを使用して暗号化するように設定する（ステップS42）。暗号方式送信手段8

bは、暗号方式決定手段8aにより決定された変更後の復号鍵と復号手段を復号方式変更手段4aへ送信する（ステップS43）。復号方式変更手段4aは、受信した復号鍵と復号手段を復号実行手段4cへ出力し、次に受信する暗号化ブロックは復号実行手段4cを使用して復号するように設定する（ステップS44）。

【0046】情報制御手段8は、送信の停止を解除し、マルチメディア情報をブロックに分割し、送信制御手段7dへブロックの送信を再開する（ステップS45）。送信制御手段7dは、受信したブロックを暗号化実行手段7cへ出力する（ステップS46）。暗号化実行手段7cは、ステップS42で出力された変更後の暗号化鍵と暗号化手段を使用て、ブロックを暗号化し、送信制御手段7dへ出力する（ステップS47）。送信制御手段7dは、暗号化されたブロックをネットワーク5を経由して受信制御手段4dへ送信する（ステップS48）。

【0047】受信制御手段4dは、ネットワーク5から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段4cへ出力する（ステップS49）。復号実行手段4cは、ステップS42で出力された復号鍵と復号手段を使用して、ブロックを復号し、受信制御手段4dへ出力する（ステップS50）。受信制御手段4dは、復号したブロックを実行制御手段3へ送信する（ステップS51）。

【0048】以上のように、この実施の形態によれば、使用する暗号方式を動的に変更することができるので、マルチメディア情報サーバに暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【0049】なお、この実施の形態では、暗号方式決定手段8aが新たな暗号方式を決定し、暗号方式送信手段8bは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段8aが暗号方式送信手段8bの機能を有し、新たな暗号方式に対応する各手段を送信するように構成することも出来る。

【0050】この実施の形態では、図10に示したように、送信手段7内の暗号化実行手段7b、7c、及び、受信手段4内の復号実行手段4b、4cは、2つに限らず、2つ以上であっても良い。一度使用した暗号化方式は、暗号化実行手段7b、7c及び復号実行手段4b、4cに保存されていて、再度同じ暗号方式が使用されるときに、新しい暗号化鍵を暗号化実行手段7b、7cへ出力し、新しい復号鍵を復号実行手段4b、4cへ出力して、暗号化実行手段7b、7c内にある暗号化手段と、復号実行手段4b、4c内にある復号手段を再使用する。

【0051】また、暗号化実行手段7b、7c、又は、復号実行手段4b、4cが既に使用中で、未使用のものがないときは、使用頻度の低い暗号化実行手段7b、7c、又は、復号実行手段4b、4cを使用するように制御する。

【0052】実施の形態7．実施の形態7は、図13に示すように、暗号化されたマルチメディア情報14bのブロックと、その暗号化に使用した暗号方式の暗号方式番号14aとによって構成される送信データ14を作成するものである。システムの構成は、実施の形態6で説明した図10のものと同様であるが、送信制御手段7dと受信制御手段4dの処理が異なる。送信制御手段7dは、図13に示した送信データを作成し、ネットワーク5を介して受信制御手段4dへ送信し、これを受信した受信制御手段4dは、暗号化されたマルチメディア情報14bを復号する復号手段を、暗号方式番号14aにより決定し、復号実行手段4b又は復号実行手段4cのいずれかに復号を実行させる。

【0053】実施の形態8．図14は、実施の形態8のマルチメディア情報システムの構成図である。図において、15はマルチメディア情報を実行するための複数の手段を実行方式番号とともに蓄積している実行方式データベースである。ユーザ情報データベース9は図2に示すものであり、マルチメディア情報データベース10は図3に示すものである。実行制御手段3は、実行情報制御手段3aと実行手段3bとから構成されている。実行手段3.bは、受信手段4により復号されたマルチメディア情報を実行し、実行結果を入出力手段2に送信する。実行情報制御手段3aは、一定時間間隔で、マルチメディア情報を実行している時の実行情報と、入出力手段2により出力されたユーザの要求とをマルチメディア情報サーバ8に送信する。実行情報には、ユーザ登録番号9b、実行中のマルチメディア情報番号10b、現在までのマルチメディア情報の実行の累積時間が含まれている。情報制御手段8は、制御手段8dとマルチメディア情報送信手段8eとから構成されている。制御手段8dは、実行情報制御手段3aにより送信されたマルチメディア情報の実行情報を受信してその情報を解析し、マルチメディア情報送信手段8eを制御する。マルチメディア情報送信手段8eは、マルチメディア情報データベース10からマルチメディア情報を取得し、送信手段7へ送信する。送信手段7は、マルチメディア情報を暗号化して受信手段4へ送信する。

【0054】次に、マルチメディア情報の実行を開始するまでの動作を図15のフローチャートに基づいて説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bとを制御手段8dへ送信する（ステップS60）。制御手段8dは、ユーザ登録番号9bを検索条件としてユーザ情報データベース9からユーザの契約情報レコード9aを取り出し、契約タイプ9eから、要求のあったマルチメディア情報を実行可能であるか、また、要求の合った日時で実行が開始できるか

15

判定する（ステップS61）。制御手段8dは、マルチメディア情報の実行開始が可能であると判定すると、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報レコード10aを取り出し、実行方式番号10dを取得する（ステップS62）。次に、制御手段8dは、実行方式番号10dを検索条件として、実行方式データベース15から実行手段を取り出し、実行情報制御手段3aへ送信する（ステップS63）。実行情報制御手段3aは、受信した実行手段を実行手段3bへ出力する（ステップS64）。制御手段8dは、マルチメディア情報送信手段8eへマルチメディア情報番号10bを出力する（ステップS65）。マルチメディア情報送信手段8eは、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報レコード10aを取り出し、ブロックに分割して送信手段7へ送信する（ステップS66）。

【0055】送信手段7は受信したブロックを暗号化し、ネットワーク5を経由して、受信手段4へ送信する（ステップS67）。受信手段4は受信したブロックを復号して、実行手段3bへ送信する（ステップS68）。実行手段3bは、実行準備が終了したメッセージを入出力手段2へ出力する（ステップS69）。ユーザは入力手段2から、マルチメディア情報の実行開始を入力する（ステップS70）。実行情報制御手段3aは、実行開始の指示を受け取ると、マルチメディア情報の実行の開始のメッセージを制御手段8dへ送信し、実行の累積時間の計数を開始する（ステップS71）。制御手段8dは、マルチメディア情報の実行の開始のメッセージを受信すると、マルチメディア情報送信手段8eへ送信開始メッセージを出力する（ステップS72）。

【0056】次に、マルチメディア情報の実行中の動作を図16のフローチャートに基づいて説明する。マルチメディア情報送信手段8eは、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報を取り出してブロックに分割し、送信手段7へ送信する（ステップS80）。制御手段8dは、マルチメディア情報の実行の累積時間の計数を開始し、実行情報の受信を待つ（ステップS81）。送信手段7は、マルチメディア情報のブロックを暗号化し、ネットワーク5を経由して、受信手段4へ送信する（ステップS82）。受信手段4は、受信したブロックを復号し、実行手段3bへ送信する（ステップS83）。実行手段3bは、受信手段4からマルチメディア情報を受信すると、マルチメディア情報を実行し、実行結果を入出力手段2へ出力する（ステップS84）。

【0057】ステップS80～S84の動作を繰り返しているときに一定時間が経過すると（ステップS85）、実行情報制御手段3aは、現在までのマルチメディア情報の実行の累積時間をセットした実行情報を制御

16

手段8dに送信する（ステップS86）。制御手段8dは、制御手段8dが計数した実行の累積時間と実行情報にセットされている累積時間との差の絶対値を計算し、その差の絶対値が制御手段8dが保有している誤差の範囲を超えているか否かをチェックし（ステップS87）、超えている場合は（ステップS88）、契約タイプ9eに一致しない不正な実行が検出されたと判断し、送信の停止を示すメッセージをマルチメディア情報送信手段8eへ出力する（ステップS88）。マルチメディア情報送信手段8eはマルチメディア情報の送信を中止する（ステップS89）。

【0058】以上のように、この実施の形態によれば、マルチメディア情報の実行累積時間を契約タイプに基づいてチェックし、所定の時間を超えているときには送信を停止するので、マルチメディア情報の実行中に、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0059】実施の形態9．図17は、実施の形態9のマルチメディア情報システムの構成図である。図において、8fは実行情報を実行情報制御手段3aから送信するタイミングを制御手段8dからの要求で決定する実行情報送信方式決定手段である。

【0060】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ情報データベース9からユーザ登録番号9bを検索条件として、ユーザの契約情報レコード9aを取り出し、契約タイプ9eを実行情報送信方式決定手段8fへ出力する。実行情報送信方式決定手段8fは、実行情報制御手段3aで使用できる実行情報送信方式の番号リストを内部に持っており、契約タイプ9eからリストの中の一つを選択し、選択した方式の方式番号を制御手段8dへ出力する。制御手段8dは、方式番号を実行情報制御手段3aへ送信する。実行情報制御手段3aは、方式番号を受信すると、実行情報を方式番号の実行情報送信方式に基づいて、制御手段8dへ送信する。

【0061】なお、実行情報の送信方式は、情報実行中にユーザの要求があった時のみ実行情報を送信する方式、ある一定の時間間隔で実行情報を送信する方式、あるいは、不規則な時間間隔で実行情報を送信する方式などがある。

【0062】以上のように、この実施の形態によれば、マルチメディア情報サーバへ実行情報を送信する方式を変更することにより、実行情報を送る時間にユーザおよび第三者が盗聴し虚の実行情報を送信することができなくなるので、不正なマルチメディア情報の実行を防止する効果がある。

【0063】実施の形態10．図18は、実施の形態10におけるユーザ情報データベースの構成図であり、図

2に示したユーザ情報データベースに対して、マルチメディア情報番号9f、9hとマルチメディア実行制御情報9g、9iとを追加し、ユーザがサービスを契約しているマルチメディア情報の番号と実行制御情報とを保持している。この実施の形態のシステム構成は、図14に示したものと同様である。

【0064】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ情報データベース9からユーザ登録番号9bを検索条件として、ユーザの契約情報レコード9aを取り出し、その中のマルチメディア情報番号9f、9hに、ユーザが要求しているマルチメディア情報番号10bが含まれているか否かを確認する。制御手段8dは、ユーザが要求している番号を見つけると、マルチメディア情報番号9f、9hに対応するマルチメディア実行制御情報9g、9iに基づいて、マルチメディア情報の実行の開始が可能であるか否かを判定する。ユーザが要求している番号がない場合は、契約タイプ9eに基づいて、要求のあったマルチメディア情報を実行可能であるか否か、また、要求のあった日時で実行の開始が可能であるか否かを判定する。

【0065】マルチメディア情報の実行中にユーザの制御要求が発生すると、実行情報制御手段3aはその要求を実行情報として、制御手段8dへ送信する。制御手段8dは、マルチメディア実行制御情報9g、9iに基づいて、この要求が実行可能であるか否かを判定する。可能であると判定されれば、実行情報制御手段3aへ実行可能であるメッセージを送信する。実行情報制御手段3aは、実行手段3bをユーザの要求に基づいて制御する。不可能であると判定されれば、実行情報制御手段3aへ実行不可であるメッセージを送信する。実行情報制御手段3aは、入出力装置1へユーザの要求は破棄されたこと示すメッセージを出力する。

【0066】以上のように、この実施の形態によれば、ユーザ情報データベース中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0067】実施の形態11．図19は、実施の形態11におけるマルチメディア情報データベースの構成図であり、図3に示したマルチメディア情報データベースに対して、マルチメディア情報の実行を制約する実行制約条件10eを追加している。この実施の形態のシステム構成は、図14に示したものと同様である。

【0068】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ登録番号9bを検索条件として、ユーザ情報データベース9からユーザの契約情報レコード9a中のユーザの契約タイプ9eを取り出す。また、制御手段8dは、マルチメディア情報番号10bを検索条件として、マルチメディア情報データベース10からマルチメディア情報レコード10a中の実行制約条件10eを取り出し、ユーザの契約タイプ9eが実行制約条件10eに含まれているか否かを確認する。含まれている場合は、契約タイプ9eから、要求のあったマルチメディア情報を実行可能であるか否か、また、要求の合った日時で実行の開始が可能であるか否かを判定する。含まれていない場合は、ユーザからの要求を破棄し、ユーザからの要求が破棄されたことを示すメッセージを実行情報制御手段3aへ送信する。実行情報制御手段3aは、入出力装置1へユーザの要求が破棄されたこと示すメッセージを出力する。

【0069】以上のように、この実施の形態によれば、マルチメディア情報データベース中にマルチメディア情報を実行するための実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0070】

【発明の効果】以上のように、請求項1記載の発明よれば、マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、ユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【0071】請求項2記載の発明によれば、複数の暗号化手段と複数の復号手段とを記憶する暗号方式記憶手段を備え、暗号化手段と復号手段とをユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【0072】請求項3記載の発明によれば、暗号化マルチメディア情報を送信する送信手段は、複数の暗号化手段を記憶する暗号方式記憶手段を備え、暗号化マルチメディア情報を復号する受信手段は、複数の復号手段を記憶する復号方式記憶手段を備えたので、復号手段をサーバからクライアントに送信する必要が無いため、復号手段の送信時間分を短縮できるという効果がある。

【0073】請求項4記載の発明によれば、暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記

憶手段を備え、ユーザとの契約情報と地域情報とに基づいて暗号化手段と復号手段とを決定するので、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択できるという効果がある。

【0074】請求項5記載の発明によれば、サーバの送信手段は、実行中でない暗号化実行手段に暗号化を実行させる暗号方式変更手段を備え、クライアントの受信手段は、実行中でない復号実行手段に復号を実行させる復号方式変更手段を備えたことにより、使用する暗号方式を動的に変更することができるので、暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【0075】請求項6記載の発明によれば、暗号化マルチメディア情報の送信データ中に使用した暗号化手段の種別を格納することにより、送信データから暗号方式を知ることができるので、暗号方式をクライアントへ通知する必要が無く、時間が短縮できるという効果がある。

【0076】請求項7記載の発明によれば、クライアント側でのマルチメディア情報の実行状態を示す実行情報をユーザとの契約情報と照合し、契約に基づいてマルチメディア情報を実行しているか否かを判別するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0077】請求項8記載の発明によれば、クライアントからサーバへの実行情報送信方式をユーザとの契約情報に基づいて決定することにより、実行情報を送る時間に盗聴し虚の実行情報を送信することができなくなるので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0078】請求項9記載の発明によれば、ユーザ情報記憶手段中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0079】請求項10記載の発明によれば、マルチメディア情報記憶手段中にマルチメディア情報の実行を制約する実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【図面の簡単な説明】

【図1】 実施の形態1のマルチメディア情報システムの構成図である。

【図2】 ユーザ情報データベースの構成図である。

【図3】 マルチメディア情報データベースの構成図である。

【図4】 暗号方式データベースの構成図である。

【図5】 実施の形態1のマルチメディア情報システムの動作を示すフローチャートである。

【図6】 実施の形態2のマルチメディア情報システムの構成図である。

【図7】 実施の形態3のマルチメディア情報システムの構成図である。

【図8】 実施の形態4のマルチメディア情報システムの構成図である。

【図9】 実施の形態5の暗号方式データベースの構成図である。

【図10】 実施の形態6のマルチメディア情報システムの構成図である。

【図11】 実施の形態6のマルチメディア情報システムの動作を示すフローチャートである。

【図12】 実施の形態6のマルチメディア情報システムにおける暗号方式を変更する場合の動作を示すフローチャートである。

【図13】 実施の形態7におけるマルチメディア情報サーバの送信データの構成図である。

【図14】 実施の形態8のマルチメディア情報システムの構成図である。

【図15】 実施の形態8のマルチメディア情報システムの動作を示すフローチャートである。

【図16】 実施の形態8のマルチメディア情報システムにおけるマルチメディア情報実行中の動作を示すフローチャートである。

【図17】 実施の形態9のマルチメディア情報システムの構成図である。

【図18】 実施の形態10におけるユーザ情報データベースの構成図である。

【図19】 実施の形態11におけるマルチメディア情報データベースの構成図である。

【図20】 従来のマルチメディア情報システムの概略構成図である。

【図21】 従来のマルチメディア情報システムにおけるメディアデータの構成図である。

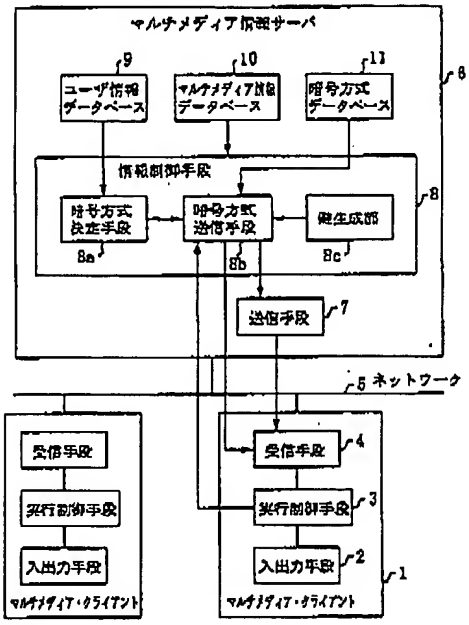
【符号の説明】

1 マルチメディア・クライアント、2 入出力手段、3 実行制御手段、3a 実行情報制御手段、3b 実行手段、4 受信手段、4a 復号方式変更手段、4b、4c 復号実行手段、4d 受信制御手段、5 ネットワーク、6 マルチメディア情報サーバ、7 送信手段、7a 暗号方式変更手段、7b、7c 暗号化実行手段、7d 送信制御手段、8 情報制御手段、8a 暗号方式決定手段、8b 暗号方式送信手段、8c 鍵生成部、8d 制御手段、8e マルチメディア情報送信手段、8f 実行情報送信方式決定手段、9 ユーザ情報データベース、9a 契約情報レコード、9b ユーザ登録番号、9c 氏名、9d 住所、9e 契約タイプ、9f マルチメディア情報番号、9g マルチメデ

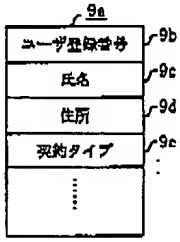
ィア実行制御情報、９ｈ　マルチメディア情報番号、９ｉ　マルチメディア実行制御情報、１０　マルチメディア情報データベース、１０ａ　マルチメディア情報レコード、１０ｂ　マルチメディア情報番号、１０ｃ　マルチメディア情報の名称、１０ｄ　実行方式番号、１０ｅ　実行制約条件、１０ｆ　マルチメディア情報、１１　暗号方式データベース、１１ａ　暗号方式レコード、１＊

＊１ｂ暗号方式番号、１１ｃ　暗号方式の名称、１１ｄ　鍵生成手段、１１ｅ　暗号化手段、１１ｆ　復号手段、１１ｇ　使用可能地域情報、１２　復号手段データベース、１３　暗号化手段データベース、１４　送信データ、１４ａ　暗号方式番号、１４ｂ　暗号化されたマルチメディア情報、１５　実行方式データベース。

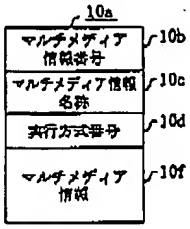
【図１】



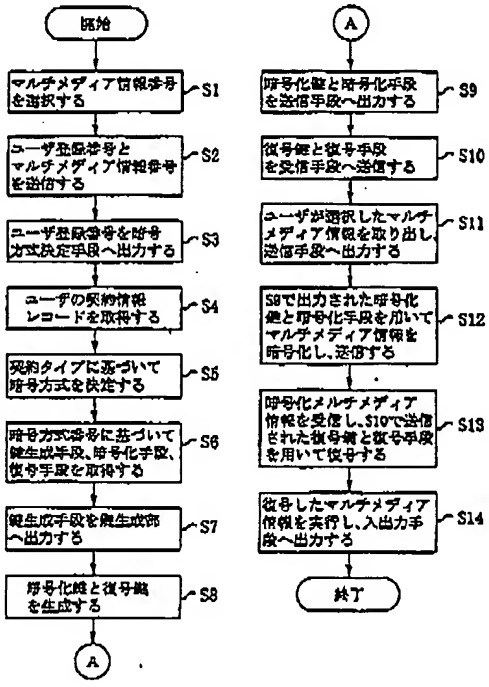
【図２】



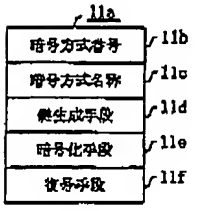
【図３】



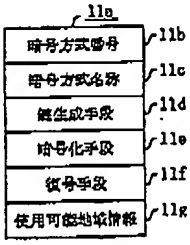
【図５】



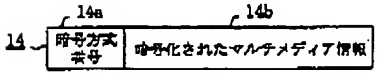
【図４】



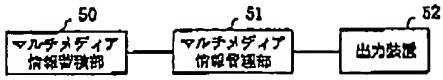
【図９】



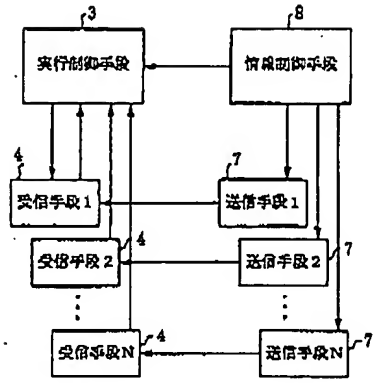
【図１３】



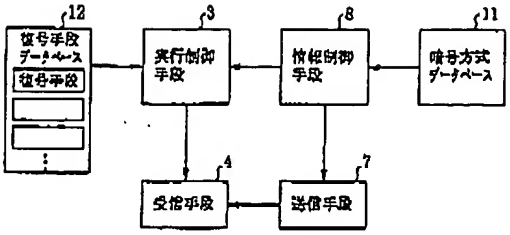
【図２０】



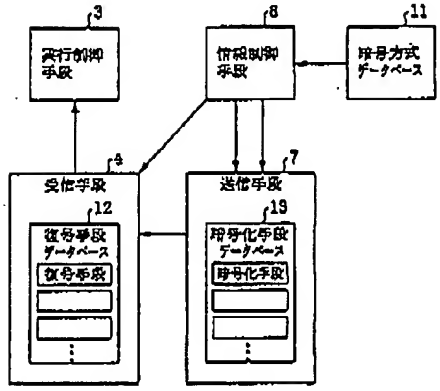
【図6】



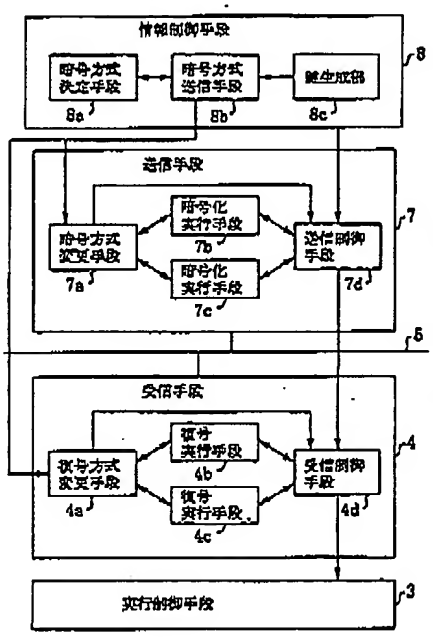
【図7】



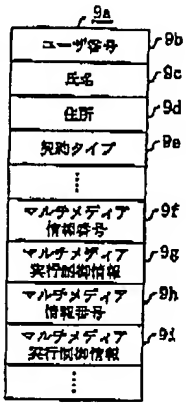
【図8】



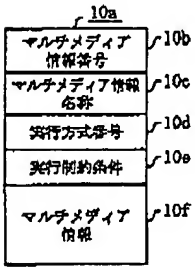
【図10】



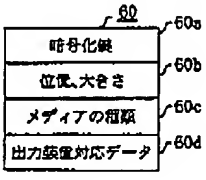
【図18】



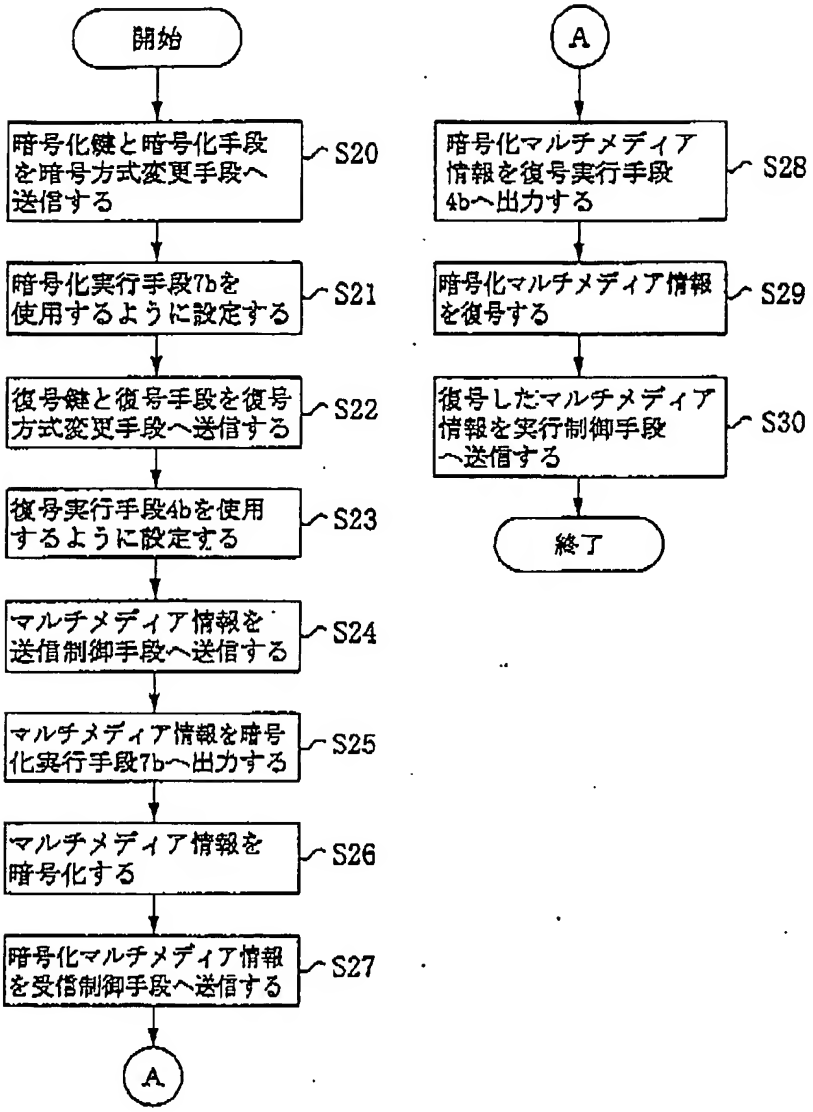
【図19】



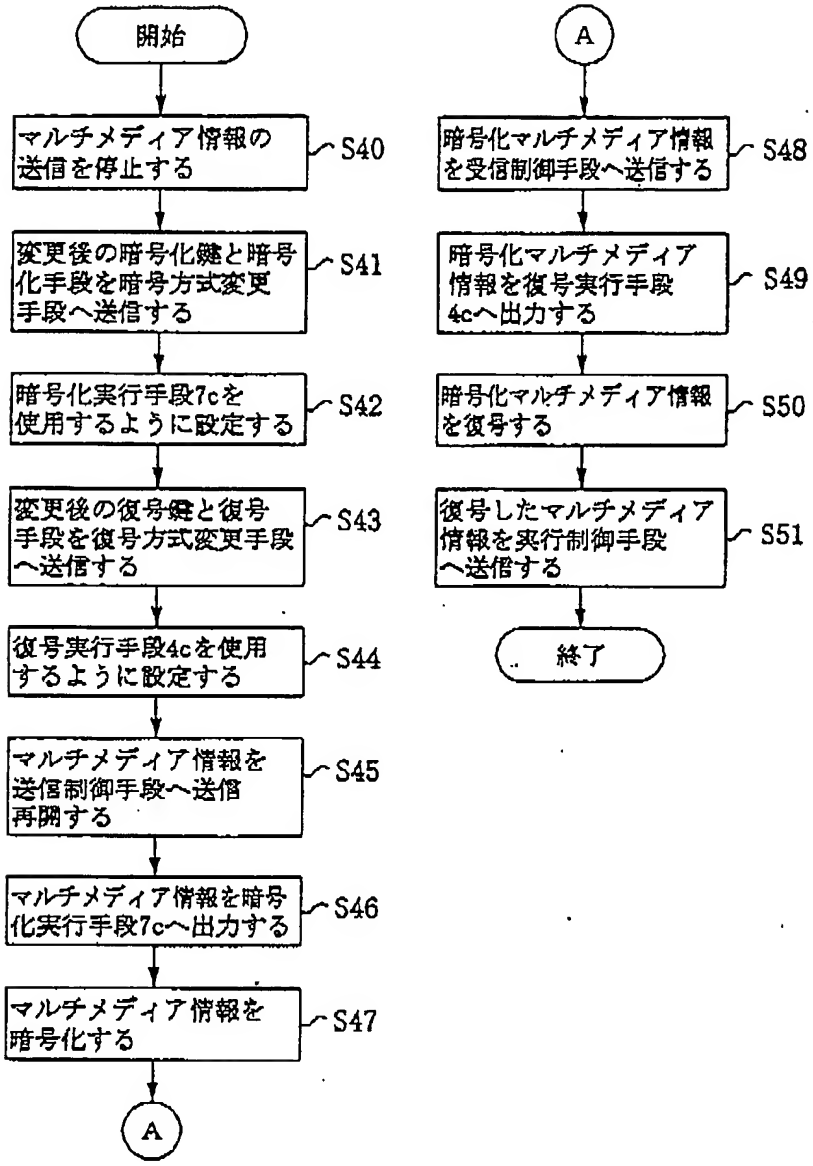
【図21】



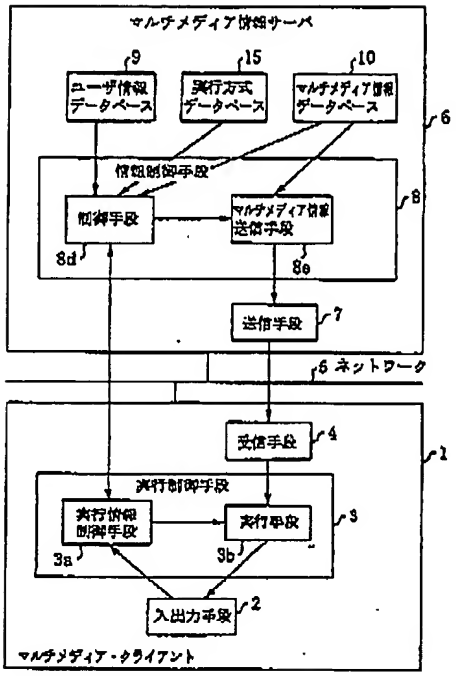
【図11】


開始
暗号化鍵と暗号化手段を暗号方式変更手段へ送信する
S20
暗号化実行手段7bを使用するように設定する
S21
復号鍵と復号手段を復号方式変更手段へ送信する
S22
復号実行手段4bを使用するように設定する
S23
マルチメディア情報を送信制御手段へ送信する
S24
マルチメディア情報を暗号化実行手段7bへ出力する
S25
マルチメディア情報を暗号化する
S26
暗号化マルチメディア情報を受信制御手段へ送信する
S27
A
A
暗号化マルチメディア情報を復号実行手段4bへ出力する
S28
暗号化マルチメディア情報を復号する
S29
復号したマルチメディア情報を実行制御手段へ送信する
S30
終了

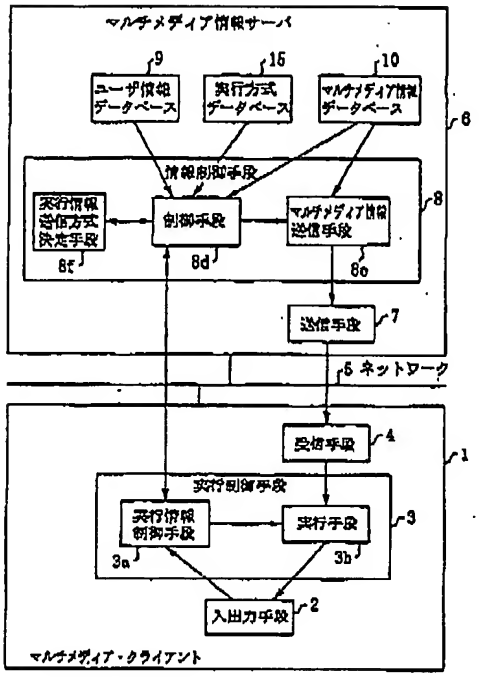
【図12】


開始
マルチメディア情報の送信を停止する
S40
変更後の暗号化鍵と暗号化手段を暗号方式変更手段へ送信する
S41
暗号化実行手段7cを使用するように設定する
S42
変更後の復号鍵と復号手段を復号方式変更手段へ送信する
S43
復号実行手段4cを使用するように設定する
S44
マルチメディア情報を送信制御手段へ送信再開する
S45
マルチメディア情報を暗号化実行手段7cへ出力する
S46
マルチメディア情報を暗号化する
S47
A
A
暗号化マルチメディア情報を受信制御手段へ送信する
S48
暗号化マルチメディア情報を復号実行手段4cへ出力する
S49
暗号化マルチメディア情報を復号する
S50
復号したマルチメディア情報を実行制御手段へ送信する
S51
終了

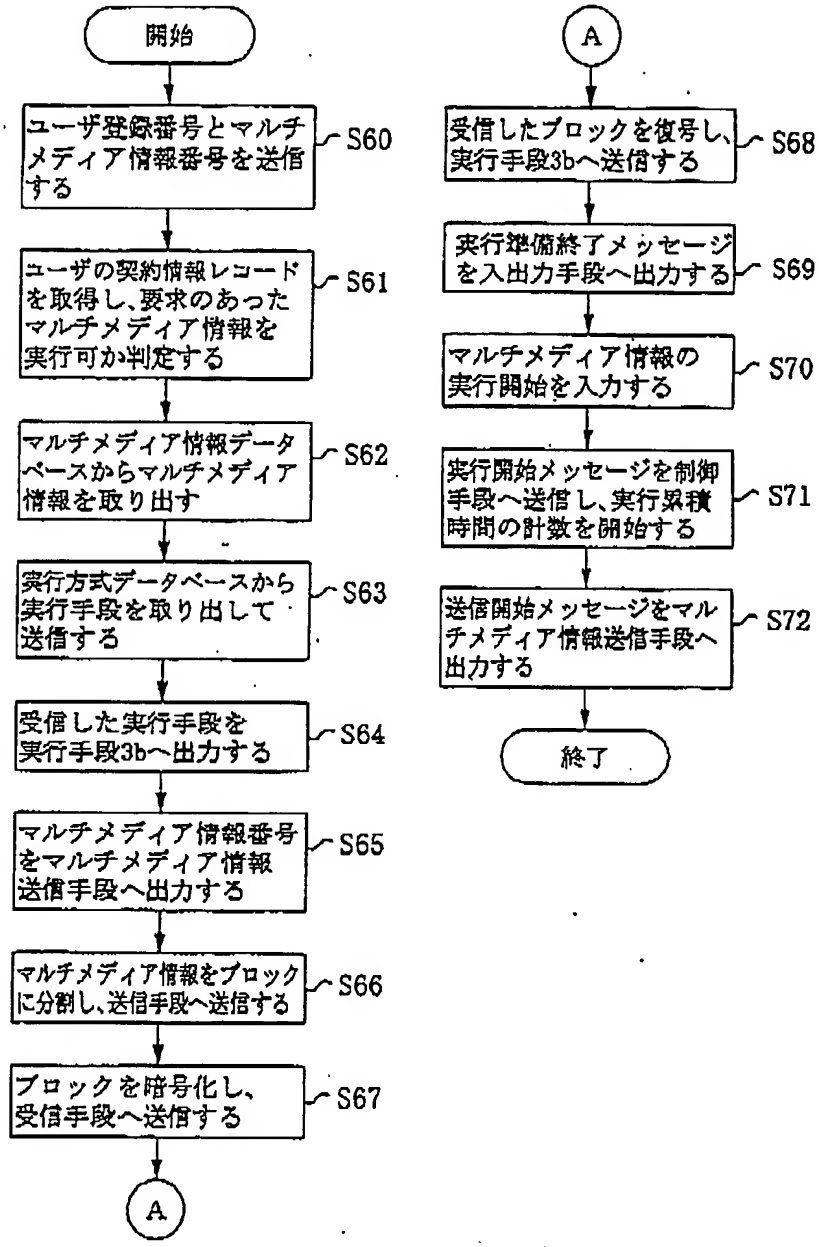
【図14】


マルチメディア情報サーバ
9
15
10
ユーザ情報データベース
実行方式データベース
マルチメディア情報データベース
6
情報制御手段
制御手段
マルチメディア情報送信手段
8
8d
8e
送信手段
7
5 ネットワーク
受信手段
4
1
実行制御手段
実行情報制御手段
実行手段
3
3a
3b
入出力手段
2
マルチメディア・クライアント

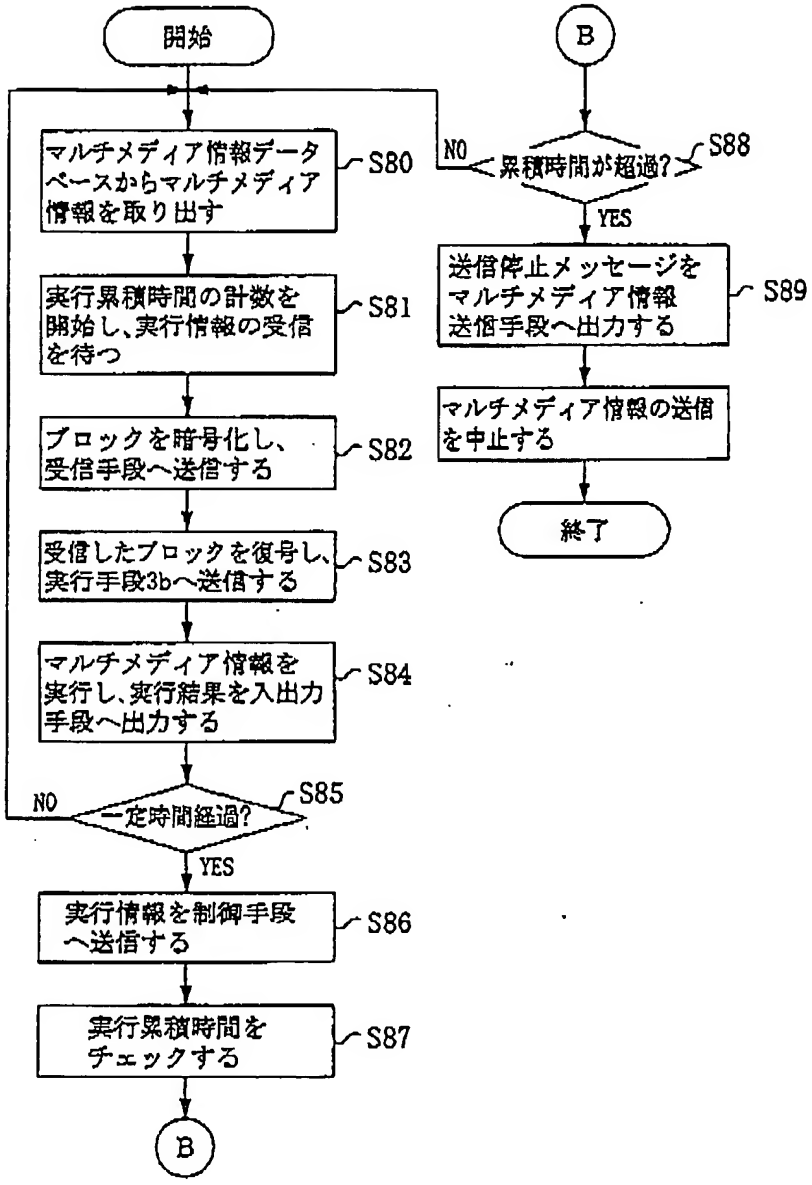
【図17】


マルチメディア情報サーバ
9
15
10
ユーザ情報データベース
実行方式データベース
マルチメディア情報データベース
6
情報制御手段
実行情報受信方式決定手段
制御手段
マルチメディア情報送信手段
8
8f
8d
8e
送信手段
7
5 ネットワーク
受信手段
4
1
実行制御手段
実行情報制御手段
実行手段
3
3a
3b
入出力手段
2
マルチメディア・クライアント

【図15】


開始
ユーザ登録番号とマルチメディア情報番号を送信する
S60
ユーザの契約情報レコードを取得し、要求のあったマルチメディア情報を実行可か判定する
S61
マルチメディア情報データベースからマルチメディア情報を取り出す
S62
実行方式データベースから実行手段を取り出して送信する
S63
受信した実行手段を実行手段3bへ出力する
S64
マルチメディア情報番号をマルチメディア情報送信手段へ出力する
S65
マルチメディア情報をブロックに分割し、送信手段へ送信する
S66
ブロックを暗号化し、受信手段へ送信する
S67
A
A
受信したブロックを復号し、実行手段3bへ送信する
S68
実行準備終了メッセージを入出力手段へ出力する
S69
マルチメディア情報の実行開始を入力する
S70
実行開始メッセージを制御手段へ送信し、実行累積時間の計数を開始する
S71
送信開始メッセージをマルチメディア情報送信手段へ出力する
S72
終了

【図16】


開始
マルチメディア情報データベースからマルチメディア情報を取り出す
S80
実行累積時間の計数を開始し、実行情報の受信を待つ
S81
ブロックを暗号化し、受信手段へ送信する
S82
受信したブロックを復号し、実行手段3bへ送信する
S83
マルチメディア情報を実行し、実行結果を入出力手段へ出力する
S84
NO
一定時間経過?
S85
YES
実行情報を制御手段へ送信する
S86
実行累積時間をチェックする
S87
B
B
NO
累積時間が超過?
S88
YES
送信停止メッセージをマルチメディア情報送信手段へ出力する
S89
マルチメディア情報の送信を中止する
終了

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.